UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/731,036	12/09/2003	Kathleen Lane	LANE-SEC-US	6726

7590 02/08/2007

PATRICK REILLY
BOX 7218
SANTA CRUZ, CA 95061-7218

EXAMINER	
NGUYEN, NAM V	
ART UNIT	PAPER NUMBER
2612	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

SF

Office Action Summary	Application No.	Applicant(s)	
	10/731,036	LANE ET AL.	
	Examiner	Art Unit	
	Nam V. Nguyen	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 10-26* is/are rejected.

7)☒ Claim(s) *8 and 9* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/7/06* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/7/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's Amendment which is filed November 7, 2006.

An amendment to the claims 1, 6-8, 10, 14, 17-18, 21-22 and 24-26 has been entered and made of record in the application of Lane et al. for a "secure personal RFID documents and method of use" filed December 09, 2003.

Claims 1-26 are pending.

Response to Arguments

The replacement drawing(s) were received on November 7, 2006. These drawing are accepted.

In view of applicant's amendment to amend the claims 1-6, 8-9, 17, 24-26 to obviate the objections and §112 rejections, therefore, examiner has withdrawn the objection and the rejection under 35 U.S.C §112, second paragraph.

Applicant's arguments with respect to claims 7 and 10-26, filed November 7, 2006 have been fully considered but are moot in view of the new ground(s) of rejection.

In response to Applicant's argument that currently amended Claims 1-6 includes and is limited too, allowable subject matter and teaches that "a change in information stored in the durable memory of the secure document may result in an automatic update of information stored in a plurality of related electronic documents by means of a communication networks" does not include certain features of Applicant's invention, the limitations on which the Applicant argues and relies above are not stated in these claims. It is the claims that define the claimed invention, and it is claims, not specifications that are anticipated or unpatentable. *Constant v. Advanced Micro-Devices Inc.,* 7 USPQ2d 1064.

Claim Objections

Claim 8 recites the limitation "the group" in line 11. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 is objected to because of the following informalities: "the group" in line 16 should be "another group". An appropriate correction is required.

Claim 8 is objected to because of the following informalities: "a primary/secondary document coupled with the first electronic memory" in lines 8 and 19 should be "a primary/secondary document includes the first electronic memory" because the memory embedded within the document, see Specification on page 39. An appropriate correction is required.

Claim 8 recites the limitation "the secondary electronic memory" in lines 19 and 20. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 is objected to because of the following informalities: "whereby a change in information related to the primary or secondary document" in line 22 should be "whereby a change in information stored in the memory related to the primary or secondary document". An appropriate correction is required.

Claim 14 recites the limitation "the group" in line 13. There is insufficient antecedent basis for this limitation in the claim.

Claim 14 is objected to because of the following informalities: "human being," in line 19 should be "human being;". An appropriate correction is required.

Claim 18 recites the limitation "the group" in line 21. There is insufficient antecedent basis for this limitation in the claim.

Claim 18 is objected to because of the following informalities: "human being," in line 7 should be "human being;". An appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yap et al. (US# 6,111,506) in view of Hopkins (US# 5,757,918).

Referring to Claim 1, Yap et al. disclose a secure document (10) (i.e. a security identification document) communicatively coupled and associated with a plurality of related electronic documents (i.e. luggage identification document or a travel authorization document) by an electronic communication network (64) (i.e. a computer) (column 1 lines 23 to 30; see Figure 7), the secure document (10) (i.e. a security identification document) containing: a flexible substrate (12) having a surface (column 12 line 28 to 39; see Figures 1 to 5), the surface visibly presenting information (column 14 lines 17 to 21); and

an integrated circuit (14) (i.e. a microprocessor) coupled with the substrate (12), the integrated circuit (14) including: a durable memory (i.e. embedded in microprocessor 14), the durable memory storing a 1st digital code (i.e. secure identification data), wherein the 1st digital code is related to a life factor (i.e. birth certificate data, driver's license data information) (column 5 lines 45 to column 6 line 33; column 12 lines 43 to 58; see Figures 1 and 7), and whereby certification for the authentication and/or accuracy of the secure document (10) is based at least partly on the 1st digital code (identification data) stored within the integrated circuit (14) (column 7 line 12 to 67; column 8 line 40 to 65; column 14 line 53 to column 16 line 54; see Figures 1 to 8),

wherein modification to information stored in the durable memory of the secure document (10) may be read by the electronic communications network (64) (i.e. a computer) (column 15 lines 6 to 37; see Figure 7) and employed to modify at least one of the plurality of related electronic documents (i.e. luggage identification document or a travel authorization document) (column 16 lines 39 to 54).

However, Yap et al. did not explicitly disclose a 2nd digital code and the 2nd digital code is an encryption code.

In the same field of endeavor of an identification transponder, Hopkins teaches that a 2nd digital code (aB) (i.e. a secret value) and the 2nd digital code is an encryption code (column 5 lines 56 to 64; see Figures 1 to 5) in order to secure the smart card reading terminal and the host computer and to avoid counterfeit card.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the secret value (aB) in smart card taught by Hopkins in an improved security identification document of Yap et al. because the secret value is not transmit to the reading terminal would avoid duplication or counterfeit of the identification of the smart card.

Referring to Claims 2, Yap et al. in view of Hopkins disclose the system and the secure document of claim 1, Yap et al. disclose wherein the life factor is related to an event of a specific human being, the event selected from the group consisting of a birth of a human being (column 4 line 2 to 24; column 14 line 8 to 37).

Referring to Claims 3, Yap et al. in view of Hopkins disclose the system and the secure document of claim 1, Yap et al. disclose wherein the life factor is related to an aspect of a specific human being, the aspect selected from the group consisting of a biometric pattern (column 4 lines 38 to 59; column 5 line 7 to 23; column 6 line 45 to 51).

Referring to Claims 4, Yap et al. in view of Hopkins disclose the system and the secure document of claim 1, Yap et al. disclose wherein the integrated circuit is an RFID (column 5 line 64 to column 6 line 16; column 7 lines 36 to 43; see Figures 1 to 7).

Referring to Claim 5, Yap et al. in view of Hopkins disclose the secure document of claim 1, Hopkins discloses wherein the 2nd digital code (aB) (i.e. a secret value) is secret key, and the key is configured for use in an encryption method (column 2 lines 62 to 65).

Referring to Claim 6, Yap et al. in view of Hopkins disclose the secure document, to the extent as claimed with respect to claim 1 above, and Yap et al. disclose further that whereby certification for authentication of the secure document (10) is based at least partly on the first digital code (i.e. secure identification data) stored within the integrated circuit (14) (column 15 lines 53 to 65).

Claims 7 and 10-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yap et al. (US# 6,111,506) in view of Hopkins (US# 5,757,918) and in further view of Moriguchi et al. (US# 6,587,756).

Referring to Claim 7, Yap et al. in view of Hopkins disclose the secure documentation system, to the extent as claimed with respect to claim 1 above, and Yat et al. further disclose an information technology system (60) (i.e. a security system) for periodically associating an identity of a specific human being to the document (10) via at least one bio-metric measurement

(72) (i.e. biometric data input device); and a security system (64) (i.e. a computer) for recording a personal identification number, or "PIN", on the document (10) and the security system (64) protecting the PIN from unauthorized reading from the document (10) (column 14 line 54 to column 16 line 11; see Figures 1 to 7).

However, Yap et al. in view of Hopkins did not explicitly disclose means for automatically updating information stored in the electronic memories of the related documents in accordance with information stored in the first memory element.

In the same field of endeavor of communication system, Moriguchi et al. teach that means for automatically updating information stored in the electronic memories (121) (i.e. storage means) of the related documents (12) (i.e. a device) in accordance with information stored in the first memory element (111) (i.e. storage medium of a communication terminal) (column 4 lines 12 to 19; column 9 lines 46 to 65; see Figure 22) in order to improve operationality of the user and easier for the user to carry out.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize setting information onto the first device can be stored automatically in the storage medium of the second device taught by Moriguchi et al. in a secure documentation system of Yap et al. in view of Hopkins because automatically update information stored in the memories of a plurality of documents would increase operationality of the system.

Referring to Claim 10, Yap et al. in view of Hopkins disclose the secure documentation system, to the extent as claimed with respect to claim 1 above, however, Yap et al. in view of Hopkins did not explicitly disclose means for automatically updating information stored in the

electronic memories of the related documents in accordance with information stored in the first memory element.

In the same field of endeavor of communication system, Moriguchi et al. teach that means for automatically updating information stored in the electronic memories (121) (i.e. storage means) of the related documents (12) (i.e. a device) in accordance with information stored in the first memory element (111) (i.e. storage medium of a communication terminal) (column 4 lines 12 to 19; column 9 lines 46 to 65; see Figure 22) in order to improve operationality of the user and easier for the user to carry out.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize setting information onto the first device can be stored automatically in the storage medium of the second device taught by Moriguchi et al. in a secure documentation system of Yap et al. in view of Hopkins because automatically update information stored in the memories of a plurality of documents would increase operationality of the system.

Referring to Claims 11-13, Yap et al. in view of Hopkins and in further view of Moriguchi et al disclose the system of claim 10, the claims 11-13 same as claims 2-4 already addressed above therefore claims 11-13 are also rejected for the same obvious reasons given with respect to claim 2-4.

Referring to Claims 14-15, 17-19 and 21-26, Yap et al. disclose a system (60) (i.e. a security system) for life events record authentication, the system (60) comprising:

a document (10) having a flexible substrate (12) and an integrated circuit (15), the flexible substrate (15) having a surface, the surface visibly presenting information (column 4 line 2 to 24; column 12 line 28 to 42; see Figures 1 to 5);

the integrated circuit (15) coupled with the substrate (12), the integrated circuit (15) including: a durable memory (i.e. embedded in microprocessor 14) containing a first information (i.e. secure identification data), wherein the first information is related to information selected from the group consisting of (i.e. biometric data) (column 4 lines 38 to 59; column 5 lines 45 to column 6 line 33; column 12 lines 43 to 58; see Figures 1 and 7),

However, Yap et al. did not explicitly disclose wherein an authentication of the document is based at least partly on the at least one secret key; wherein access to the first information requires the use of the secret key; and wherein the secret key may be communicated by private means from a first agency to a second agency and the secret key may be used to delegate authority from the first authority to the second authority and means for automatically updating information stored in the electronic memories of the related documents in accordance with information stored in the first memory element.

In the same field of endeavor of a portable security device, Hopkins discloses an authentication of the document (12) (i.e. a smart card) is based at least partly on the at least one secret key (aB) (i.e. a secret value) (column 2 line 45 to 67; see Figures 1 and 2); wherein access to the first information (U) (i.e. public information) requires the use of the secret key (U) (column 3 lines 1 to 60; see Figure 1); and wherein the secret key (U) may be communicated by private means (26) from a first agency (20) (i.e. a card issuer site) to a second agency (22) (i.e. a

terminal) and the secret key (U) may be used to delegate authority from the first authority (20) to secure verification and authentication system.

One of ordinary skilled in the art recognizes the need for the terminal to verify the smart card by a secret value taught by Hopkins in a security identification document of Yap et al. because Yap et al. suggest it is desired to provide that the memory in the document with a RFID integrated circuit can be used to store a plurality of security identification data of a user (column 5 line 45 to 68; column 6 line 45 to 67) and Hopkins teaches that a terminal verifies the smart card for counterfeit and that the user is authorized by the value of secret key (column 5 line 1 to column 6 line 65; see Figures 1 to 3) in order to improve security at the terminal for verifying a smart card and the user. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to have a the terminal to verify the smart card by a secret value taught by Hopkins in a security identification document of Yap et al. with the motivation for doing so would have been to provide a secure communicating in each of the cards in a programmable security identification document.

In the same field of endeavor of communication system, Moriguchi et al. teach that means for automatically updating information stored in the electronic memories (121) (i.e. storage means) of the related documents (12) (i.e. a device) in accordance with information stored in the first memory element (111) (i.e. storage medium of a communication terminal) (column 4 lines 12 to 19; column 9 lines 46 to 65; see Figure 22) in order to improve operationality of the user and easier for the user to carry out.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize setting information onto the first device can be stored automatically in the

storage medium of the second device taught by Moriguchi et al. in a secure documentation system of Yap et al. in view of Hopkins because automatically update information stored in the memories of a plurality of documents would increase operationality of the system.

Referring to Claims 16 and 20, Yap et al. in view of Hopkins and Moriguchi et al. disclose the system and the secure document of claims 14 and 18, Yap et al. disclose wherein the integrated circuit is an RFID (column 5 line 64 to column 6 line 16; column 7 lines 36 to 43; see Figures 1 to 7).

Allowable Subject Matter

Claims 8-9 would be allowable if rewritten to overcome the objection, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Referring to claim 8, the following is a statement of reasons for the indication of allowable subject matter: the prior art fail to suggest wherein the secondary digital code is associated with the primary document, and wherein the primary document and secondary digital code are permanently associable with each other, and whereby a change in information stored in the memory related to the primary or secondary document may direct the communications network to automatically update information stored within electronic memories of a plurality of documents that are associated by the electronic communications network to either the primary or the secondary document.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 571-272-3061. The examiner can normally be reached on Mon-Fri, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wendy Garber can be reached on 571- 272-7308. The fax phone numbers for the organization where this application or proceeding is assigned are 571-273-8300 for regular communications.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nam Nguyen
February 5, 2007

BRIAN ZIMMERMAN
PRIMARY EXAMINER